(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－515612
（P2001－515612A）
(43)公表日　平成13年９月18日(2001.9.18)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ

審査請求　未請求　予備審査請求　有　（全 42 頁）

(21)出願番号　特願平11－535884
(86)(22)出願日　平成10年12月28日(1998.12.28)
(85)翻訳文提出日　平成11年８月31日(1999.8.31)
(86)国際出願番号　ＰＣＴ／ＩＢ９８／０２１２０
(87)国際公開番号　ＷＯ９９／３５７８５
(87)国際公開日　平成11年７月15日(1999.7.15)
(31)優先権主張番号　０９／００２，０９８
(32)優先日　平成９年12月31日(1997.12.31)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＣＮ，ＪＰ，ＫＲ

(71)出願人　コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(72)発明者　エプシュタイン　ミハエル
オランダ国　5656　アーアー　アインドーフェン　プロフ　ホルストラーン　6
(74)代理人　弁理士　杉村　暁秀　（外２名）

(54)【発明の名称】　デジタル署名を有する改訂の送信

(57)【要約】
コンピュータネットワークにおいて、文書を発生させ、文書をハッシュしてフィンガープリントを発生させ、フィンガープリントを暗号化して文書を署名し、文書の署名をユーザ装置からセキュアコンピュータ装置に送信する。セキュアコンピュータ装置は、文書の署名及びデジタル時間を有するタイムスタンプを形成する。セキュア装置は、タイムスタンプを署名してその起点を確認する。タイムスタンプ及び公証人の署名をセキュア装置からユーザの装置に送信する。ユーザは、タイムスタンプが真正であるか否かを決定するのに用いられる公証人の公開かぎに対するアクセスを有する。その後、文書が改訂され、改訂された文書がハッシュされ、改訂が元の文書に関連することの表示をハッシュに結合する。表示を、元の文書のハッシュ、元の文書の署名、元の文書に対する公証人のタイムスタンプ又は元の文書に対する公証人の署名とすることができる。

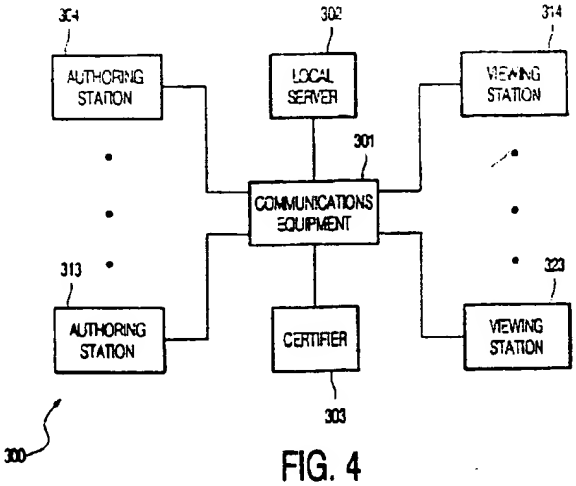

FIG. 4

【特許請求の範囲】

1．コンピュータネットワークであって、

そのコンピュータネットワークが、前記ネットワークにユーザアクセスを行うユーザコンピュータ装置を具え、そのユーザコンピュータ装置が、

元の文書を発生させる手段と、

その元の文書から文書の署名を発生させる手段と、

前記元の文書の署名を送信する手段とを有し、

前記コンピュータネットワークが、セキュアコンピュータ装置を更に具え、そのセキュアコンピュータ装置が、

前記ユーザ装置から文書の署名を受信する手段と、

前記文書の署名及び前記文書を受信したデジタル時間を有するタイムスタンプを発生させる手段と、

前記タイムスタンプを前記ユーザ装置に送信する手段とを有し、

前記ユーザシステムが、

前記元の文書に対するタイムスタンプを受信し及び格納する手段と、

前記元の文書を改訂して、改訂した文書を発生させる手段と、

前記改訂した文書に応じて改訂した文書の署名を発生させる手段とを更に有し、

前記文書の署名を送信する手段を、前記改訂した文書の署名を送信するように適合させ、

前記コンピュータネットワークが、タイムスタンプを認証する手段を更に有するコンピュータネットワークにおいて、

前記改訂した文書の署名が、前記元の書面に対するタイムスタンプにも依存するようにしたことを特徴とするコンピュータネットワーク。

2．前記タイムスタンプを証明する手段が、

前記セキュアシステムでデータを暗号化する専用かぎと、

その専用かぎを用いて以前に暗号化したデータを解読することができる公衆かぎと、

前記信頼システムで前記公開かぎを用いて前記タイムスタンプからタイム

スタンプの署名を発生させる手段と、

前記タイムスタンプの署名を前記ユーザシステムに送信する手段と、

前記ユーザ装置で公開かぎを用いて前記タイムスタンプの署名を解読する手段と、

前記タイムスタンプ又はタイムスタンプのハッシュと、前記ユーザ装置で解読されたタイムスタンプの署名とを比較して、前記タイムスタンプが真正であるか否かを決定する手段とを有することを特徴とする請求の範囲1記載のコンピュータネットワーク。

3．前記タイムスタンプを認証する手段が、

前記セキュア装置にタイムスタンプを格納するセキュア記憶装置と、

前記ユーザ装置から前記セキュア装置に前記タイムスタンプを送信する手段と、

前記セキュア装置の前記セキュア記憶装置から前記タイムスタンプを検索する手段と、

検索した前記タイムスタンプと送信されたタイムスタンプとを比較する手段と、

前記比較に依存して、前記セキュア装置から前記ユーザ装置に認証又は不認証信号を送信する手段とを有することを特徴とする請求の範囲1記載のコンピュータネットワーク。

4．前記タイムスタンプを認証する手段が、

前記セキュア装置で公開かぎを用いて前記タイムスタンプから第1のタイムスタンプの署名を発生させる手段と、

前記タイムスタンプ及び第1のタイムスタンプの署名を前記ユーザ装置に送信する手段と、

前記タイムスタンプを前記セキュア装置に戻す手段と、

前記セキュア装置に戻されたタイムスタンプから第2のタイムスタンプの署名を発生させる手段と、

前記第2のタイムスタンプの署名を前記ユーザ装置に送信する手段と、

前記第1のタイムスタンプの署名と第2のタイムスタンプの署名とを比較して

、前記タイムスタンプの真正を確認する手段とを有することを特徴とする請求の範囲１記載のコンピュータネットワーク。

５．前記セキュアサーバからの送信が、前のタイムスタンプ及びタイムスタンプの署名と、次のタイムスタンプ及びタイムスタンプの署名とを有し、各タイムスタンプが顧客識別を有し、

前記ユーザ装置が、前記前の及び次のタイムスタンプ及び署名を格納し、

前記タイムスタンプを認証する手段を、前記次のタイムスタンプを識別した顧客と通信するとともに、次の顧客から前記タイムスタンプ及びタイムスタンプの署名のコピーを得るように適合させたことを特徴とする請求の範囲１記載のコンピュータネットワーク。

６．前記文書を改訂する手段が、前記文書の受信に応答して自動的に前記文書を改訂するようにしたことを特徴とする請求の範囲１記載のコンピュータネットワーク。

７．前記ユーザコンピュータ装置が、前記文書を発生させる作成ワークステーションと、前記文書、文書の署名及び文書のタイムスタンプを格納するセキュアサーバとを有することを特徴とする請求の範囲１記載のコンピュータネットワーク。

８．元の文書を発生させる手段と、

その元の文書から文書の署名を発生させる手段と、

前記元の文書を改訂して、改訂した文書を発生させる手段と、

前記改訂した文書に依存して改訂した文書の署名を発生させる手段とを具えるコンピュータ装置において、

前記改訂した文書の署名が前記元の文書の署名にも依存するようにしたことを特徴とするコンピュータ装置。

９．タイムスタンプ処理を行うために前記元の文書をセキュアコンピュータ装置に送信する手段と、

前記セキュアコンピュータ装置が、前記元の文書に対するタイムスタンプを受信し及びそれを格納する手段とを有し、前記タイムスタンプが、元の文書の署名と

、前記タイムスタンプを発生させた際に表すデジタルスタンプ時間を有し、
前記改訂した文書の署名が、前記元の文書に対するタイムスタンプのデジタルスタンプ時間に依存するようにしたことを特徴とする請求の範囲８記載のコンピュータ装置。

１０．作者に対して、ユーザがアクセス可能な局で元の文書を形成する手段と、
前記元の文書をセキュアサーバに送信する手段と、
前記元の署名に対する署名を発生させる手段と、
前記署名を用いて、前記文書が変更されなかったをとを証明するとともに前記ユーザ又は局を識別する手段と、
前記セキュアサーバから公証人に前記元の文書の署名を送信する手段と、
前記元の文書の署名及び前記署名を前記公証人によって受信した時間を表すデジタル時間を有する公証人のタイムスタンプを発生させる手段と、
前記タイムスタンプを前記セキュアサーバに送信する手段と、
前記タイムスタンプが真正であることを確認する手段と、
前記元の文書を改訂する手段と、
改訂した文書に対する署名を前記改訂した文書に依存して発生させる手段とを具えるコンピュータネットワークにおいて、
前記改訂した文書に対する署名が前記元の文書にも依存して、前記改訂した文書が前記元の文書の積となることを確認できるようにしたことを特徴とするコンピュータネットワーク。
１１．コンピュータネットワークを操作する方法であって、
ユーザ装置に元の文書を提供するステップと、
前記元の文書に依存して、改訂した文書を発生させるステップと、
前記改訂した文書をハッシュして、文書フィンガープリントを発生させるとともに、その文書フィンガープリントを用いて、改訂した文書の署名を発生させるステップと、
前記改訂した文書の署名を、前記ユーザ装置からセキュアコンピュータ装置に送信するステップと、

改訂した文書に対するタイムスタンプを発生させ、そのタイムスタンプが、前記改訂した文書の署名と、前記タイムスタンプを発生させたときを表すデジタル時間とを有するステップと、

前記セキュア装置から前記ユーザ装置に前記タイムスタンプを送信し、前記タイムスタンプが、前記改訂した文書の署名を有するステップと、

前記タイムスタンプが真正であるか否かを決定するステップと、

前記タイムスタンプの改訂した文書の署名が真正であるか否かを、前記改訂した文書の解読と前記改訂した文書のハッシュとの間の一致に依存して決定するステップとを具える方法において、

前記文書のフィンガープリントを発生させるステップが、前記改訂した文書を前記元の文書から発生させたことを表す情報とともに前記改訂した文書をハッシュするステップを有し、前記改訂した文書の署名が真正であるか否かを決定するステップが、前記文書のフィンガープリントを再び形成する情報を表す元の文書とともに前記改訂した文書をハッシュする前記元の文書から、前記改訂した文書を発生させるか否かを決定するステップを有することを特徴とする方法。

１２．前記タイムスタンプが真正であるか否かを決定するステップが、

前記セキュア装置のセキュア記憶装置に前記タイムスタンプを格納するステップと、

前記タイムスタンプを前記ユーザ装置及びセキュア装置から送信するステップと、

前記ユーザ装置からのタイムスタンプを前記セキュア記憶装置のタイムスタンプと比較するステップと、

前記比較の結果を前記ユーザ装置に送信するステップと、

前記比較の結果に依存して前記タイムスタンプが真正であるか否かを決定するステップとを有することを特徴とする請求の範囲第１１項記載の方法。

１３．前記タイムスタンプが真正であるか否かを決定するステップが、

前記セキュア装置のセキュア記憶装置に前記タイムスタンプを格納するステップと、

前記タイムスタンプを前記ユーザ装置から前記セキュア装置に送信するステップと、

前記ユーザ装置からのタイムスタンプと前記セキュア記憶装置のタイムスタンプと比較するステップと、

前記比較の結果を前記ユーザ装置に送信するステップと、

前記タイムスタンプが真正であるか否かを前記比較の結果に依存して決定するステップとを有することを特徴とする請求の範囲１１記載の方法。

１３．前記タイムスタンプが真正であるか否かを決定するステップが、

前記セキュア装置に公開かぎを提供するステップと、

前記タイムスタンプを暗号化して、前記セキュア装置にタイムスタンプの署名を発生させる手段と、

前記タイムスタンプの署名を前記セキュア装置から前記ユーザ装置に送信するステップと、

前記タイムスタンプ及びタイムスタンプの署名を前記ユーザ装置から前記セキュア装置に送信するステップと、

前記公開かぎを用いて前記タイムスタンプを暗号化して、タイムスタンプ検査署名を発生させるステップと、

前記タイムスタンプの署名と前記タイムスタンプ検査署名とを比較するステップと、

前記タイムスタンプが真正であるか否かを前記比較の結果に依存して決定するステップとを有することを特徴とする請求の範囲１１記載の方法。

１４．前記タイムスタンプが真正であるか否かを決定するステップが、

前記セキュア装置に専用かぎを提供するステップと、

前記タイムスタンプを暗号化し、前記セキュア装置の専用かぎを用いてタイムスタンプの署名を発生させるステップと、

前記タイムスタンプの署名を前記セキュア装置から前記ユーザ装置に送信するステップと、

前記専用かぎに対する公開かぎを前記ユーザ装置に提供するステップと、

前記公開かぎを用いて前記タイムスタンプの署名を解読するステップと、

解読した前記タイムスタンプの署名と、前記タイムスタンプ又は前記タイムスタンプの処理結果とを比較するステップと、

前記タイムスタンプが真正であるか否かを前記比較に依存して決定するステップとをう有することを特徴とする請求の範囲１１記載の方法。

１５．前記タイムスタンプが真正であるか否かを決定するステップが、

次のタイムスタンプの顧客を識別する情報を前記ユーザ装置に送信するステップと、

前記改訂した文書に対するタイムスタンプを次の顧客に送信するステップと、

前記次の顧客と通信して、前記改訂した文書に対するタイムスタンプと、前記次の顧客に送信した前記改訂した文書に対するタイムスタンプとを比較するステップとを有することを特徴とする請求の範囲１１記載の方法。

１６．前記改訂した文書のフィンガープリントを発生させるステップが、前記改訂した文書の起点を表す情報とともに前記改訂した文書をハッシュするステップを有し、

前記改訂した文書の署名が真正であるか否かを決定するステップが、前記改訂した文書とともにハッシュされ、かつ、前記文書のフィンガープリントを再び形成する情報を表す起点に、前記改訂した文書が起因するか否かを決定するステップを有することを特徴とする請求の範囲１１記載の方法。

１７．情報を表す前記元の文書が、前記元の文書の署名に依存することを特徴とする請求の範囲１１記載の方法。

１８．情報を表す前記元の文書が、前記元の文書の起点に依存することを特徴とする請求の範囲１１記載の方法。

１９．前記元の文書に対するタイムスタンプを得るステップを具え、

情報を表す前記起点が、前記元の文書に対するタイムスタンプの初期時間に依存することを特徴とする請求の範囲１１記載の方法。

２０．前記改訂した文書の改訂の作者の識別を表す情報が、前記改訂のハッシュに含まれ、

前記改訂した文書の署名が真正であるか否かを決定するステップが、情報を識別する作者を有する改訂した文書をハッシュするステップを有することを特徴とする請求の範囲１１記載の方法。

２１．文書を改訂するに当たり、

前記文書、文書のタイムスタンプ及び前記文書に対するタイムスタンプの署名をセキュア装置から改訂者がアクセス可能な装置に送信するステップと、

公証人の公開かぎを使用して、前記タイムスタンプ及び署名を前記タイムスタンプにリストされた公証人によって発生させたこと及び前記タイムスタンプが変更されていないことを自動的に確認するステップと、

発生者の公開かぎを使用して、前記タイムスタンプの文書の署名を前記発生者によって発生させたこと及び前記署名を発生させたために前記文書が変更されていないことを自動的に確認するステップと、

前記確認に応じて前記文書を改訂するステップと、

前記改訂した文書を前記改訂者がアクセス可能な装置から前記セキュアサーバに送信するステップと、

前記改訂の発生者の専用かぎを使用して、前記改訂した文書に対する署名を発生させるステップと、

前記改訂した文書の署名を公証人に送信するステップと、

前記改訂した文書及び前記改訂した文書が前記公証人によって受信されたときを表すタイムスタンプを有する改訂した文書のタイムスタンプを発生させるステップと、

前記公証人の公開かぎを使用して、前記改訂した文書のタイムスタンプに対する署名を発生させるステップと、

前記タイムスタンプ及び前記改訂した文書に対するタイムスタンプの署名を前記サーバに戻すステップと、

前記改訂した文書、前記改訂した文書のタイムスタンプ及び前記改訂した文書のタイムスタンプの署名を前記セキュアサーバのセキュア記憶装置に格納するステップとを具えることを特徴とする方法。

２２．文書を自動的に改訂するに当たり、

元の文書を作成装置から顧客の装置に送信するステップと、

前記改訂した文書を前記顧客の装置に格納するステップと、

公開かぎを使用して、前記改訂した文書に対する署名と、前記改訂した文書が前記元の文書の積であり、前記顧客によって発生させ、かつ、改訂が署名されているために変更されていないことを確認する情報とを発生させるステップと、

前記改訂した文書の署名を前記顧客の装置から電子公証装置に送信するステップと、

前記改訂した文書の署名及び前記文書が公証人によって受信されたときを表すデジタル時間を有する改訂した文書に対するタイムスタンプの記録を発生させるステップと、

前記公証人の個人かぎを用いて前記タイムスタンプを暗号化し、前記タイムスタンプに対するデジタル署名を発生させるステップと、

前記タイムスタンプ及びタイムスタンプの署名を前記電子公証装置に格納するステップと、

前記タイムスタンプ及びタイムスタンプの署名を前記顧客に送信するステップと、

前記タイムスタンプ及びタイムスタンプの署名を前記顧客の装置に格納するステップとを具えることを特徴とする方法。

【発明の詳細な説明】

デジタル署名を有する改訂の送信

発明の分野

本発明は、暗号手法の分野に関するものであり、より詳しくは、所定の時間に存在を証明する暗号手法的な文書の刻時に関するものである。

発明の背景

多数の日常的な状況において、人々は、所定の日付に存在したデジタル文書(すなわち、コンピュータ装置にデジタル的に格納した文書)を確認する必要がある。すなわち、申し立てられた所定の日付や文書の送信日のような所定の日付から誰もデジタル文書を変更すなわち改訂しなかったことを証明する必要がある。

このような証明を行う方法の一つは、電子公証又は刻時として既知である。文書の一方向ハッシュを発生させ、文書の所有者の公開かぎを用いてハッシュを暗号化して、いわゆるデジタル署名を形成する。文書の署名は、デジタル署名にデジタル時間（時間及び日付のデジタル表示）を結合してタイムスタンプを形成するデジタル公証部又はタイムスタンパに送信され、タイムスタンプをハッシュし、かつ、デジタル公証部の公開かぎを用いることによってタイムスタンプのハッシュを暗号化して、タイムスタンプの署名と称される他のデジタル署名を形成する。その後、公証人は、タイムスタンプ及びタイムスタンプの署名を有する証明を作者に送信する。公証人の公開かぎを有する者は、タイムスタンプの署名を解読するとともに、結果を作者の署名及び証明の時間のハッシュと比較して、証明が行われたときに作者の署名が存在したこと及びサーバの署名及び証明の時間が公証人の個人かぎにアクセスした者によって元々互いに暗号化されていたことを証明する。

デジタル文書の公証は米国特許第５，１３６，６４６号に開示されている。装置のセキュアハードウェアによる公証は、米国特許第５，００１，７５２号に開示されている。公開かぎの暗号手法は、１９７６年１１月のＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ Ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ，Ｖｏｌ ＩＴ－２

2の644－654ページのDiffie及びHellmanによる“New Direction in Cryptography”，Rivestに対する米国特許第4，405，829号及び米国特許第4，868，877号に開示されている。一方向ハッシングは、1988年のAdvances in Cryptology－Eurocrypt'87，Springer－Verlag，LNCS，vol．304の203－217ページの“Collision－Free Has Functions and Public Key Signature Schemes”に開示されている。

上記文献を参照することによってここに組み込む。

発明の要約

本発明の目的は、改訂の証明用の方法及び装置を提供することである。

ここに開示した発明において、元の文書及び元の文書から取り出した改訂した文書を、元の文書と改訂した文書との間の関係を改訂の発生及び改訂の公証の時間とともに証明できるように署名し及び公証する。

本発明の一例において、元の文書を署名及び公証し、文書を改訂し、改訂及び元の文書との関係を署名し及び公証する。他の例において、元の文書及び自動的に発生した文書の改訂を同時に署名し及び公証する。これによって、出所及び情報の損失圧縮のような自動的に発生した改訂の発生時間の証明を許容する。

出願任の発明の他の例及び利点を、添付図面を参照して詳細に説明する。

図面の簡単な説明

図1a－1dは、改訂を証明する本発明の特定の例のフローチャートを示す。

図2a－1dは、改訂を証明する本発明の他の特定の例のフローチャートを示す。

図3a－3cは、改訂を証明する本発明の他の特定の例のフローチャートを示す。

図4は、本発明のネットワークシステムのサンプル例を示す。

図5は、図4の作成局の詳細を示す。

図6は、図4のセキュアサーバの詳細を示す

図7は、図1の公証人のホストの詳細を示す

図８は、図３のシステムをプログラムする装置の特定の例を示す。

好適な実施の形態の詳細な説明

図１ａ－１ｄは、改訂を確認する本発明の特定の実施の形態を示す。図１ａは、他者が文書のオリジンを確認できるように作者のワークステーションにロードされたソフトウェアがデジタル文書を作成し及び信号送信する方法の第１グループのステップ１００を示す。作者は、デジタル情報を暗号化することができる専用かぎを有し、他の関係者は、情報を解読することができる公開かぎを有する。すなわち、作者は、例えばサーバ上で公に利用できる公開かぎを作り、この場合、報告書（例えば、作者が創作した報告書）のオリジン又は報告書の保全性（すなわち、署名されていないために報告書が変更されていない。）を確認する他者は、報告書及び公開かぎにアクセスすることができる。本発明のこの第１部において、ステップ１０２では、作者は、ネットワークのサーバに接続されたワークステーションにロードされたソフトウェアを用いて報告書（デジタル文書）を作成し、作者は、コマンドを入力して報告書をサーバに提出する。

報告書は、作者に起因するのを証明することを任意の人が所望する情報のタイプを有し、変更されない。ステップ１０３において、作者のワークステーションは、特定の１方向ハッシング方法を用いて報告書をハッシュする。一方向ハッシュの利点は、文書を復号化するために逆転することができないことであり、その結果、文書が秘密すなわち専用であっても、ハッシュを秘密に保持する必要がない。ステップ１０４において、ワークステーションは、作者の専用かぎ（又はワークステーションの専用かぎ）を用いてハッシュを暗号化して、報告書の作者の署名を形成する。暗号化の目的は、作者が報告書の発議者であり、かつ、報告書が他者によって変更されてないのを証明することである。ハッシュの暗号化は、データ及びハッシュの秘密を保持するようなことを何も行わず、保全性及び起点を証明するだけである。報告書は、題名、作者名、ワークステーションＩＤ及び作成時間のような他の情報を有し又は関連させることができる。ワークステーションは、所望の場合には報告書、ハッシュ及び署名をワークステーション内で関連して保持することができる。ここで、「関連して」とは、報告書をハッシュ及び署名に関連させるとともにその逆もワークステーション内に格納されることを

意

味する。ステップ１０６において、ワークステーションは、作者の識別、報告書の題名、報告書及び報告書に対する作者の署名を顧客のサーバに送出（送信）する。報告書の内容が秘密すなわち専用である場合、送信前に秘密の接続がワークステーションとサーバとの間に形成され、サーバは安全なサーバとなる。ステップ１０７において、サーバは報告書をハッシュし、作者の公開かぎを用いて作者の署名を解読する。その後、サーバは、報告書のハッシュと解読された署名とを比較して、これらの整合を確認する。これらが整合している場合、サーバは、署名及び報告書が作者（又は少なくとも作者の専用かぎにアクセスすることができるもの）からのものであることを知る。その理由は、それが署名を解読した作者の公開かぎだからである。サーバは、作者が報告書を署名したために署名及び報告書が変更されていないことも知る。ステップ１０８において、サーバは、報告書、作者の識別（ＩＤ）及び作者の署名をサーバの格納部に関連して格納する。ここでも、「関連して（すなわち関連的に）格納する」とは、情報の関連の要素を互いに関連させて格納することを意味する。

次のグループの図１ｂのステップ１１０において、サーバは、報告書に対するタイムスタンプを得るとともに、そのタイムスタンプを報告書に関連させて格納する。ステップ１２２において、サーバは、作者の署名をネットワークを通じて公証部のホストシステムに送出する。公証部を、サーバのハードウェアのセキュア部とすることができ、例えば、サーバの所有者が知らないすなわち破壊することなく発見することができない専用かぎを有する装置とすることができる。署名が秘密でないので、署名送信の際に高度な安全性が要求されない。ステップ１１３において、ホストは、作者の署名、受信時間、公証人ＩＤ、シーケンス番号及び顧客ＩＤを有するタイムスタンプを作成する。ステップ１１４において、公証部はタイムスタンプをハッシュする。ステップ１１５において、公証部は、公証部の専用キーを用いてタイムスタンプのハッシュを署名する。ステップ１１６において、公証部はタイムスタンプを報告書に関連する公証部の署名と関連する。ステップ１１７において、公証部は、サーバにタイムスタンプ及び公証部の署名

を送信する。また、１個以上の前の及び／又は後のタイムスタンプをパッケージにして顧客のサーバに送信し、タイムスタンプで識別される他の顧客にコンタクトすることによって、タイムスタンプの近似時間を独立して確認することができる。ステップ１１８において、公証部の署名を確認するために、サーバは、タイムスタンプをハッシュするとともに、公証部の公開キーを用いて公証部の署名を解読する。ステップ１１９において、サーバは結果を比較し、整合がある場合にはタイムスタンプが確認される。すなわち、サーバは、タイムスタンプ及び公証部の署名が公証部からのものであり、それらが変更されていないことを知る。ステップ１２０において、サーバは、タイムスタンプと、公証部の署名と、報告書に関連する任意の前の及び／又は後のタイムスタンプを格納する。

次のグループの図１ｃのステップ１２０において、改訂者（人間のユーザ）は、改訂に対する報告書（元の文書）のコピーを得るとともに、その起点及び保全性を確認する。ステップ１２２において、改訂者は、サーバーから元の報告書を要求する。別のマテリアルを追加したり誤りを補正したりするような誰かが文書を改訂することを必要とする多数の状況がある。好適には、改訂者は、報告書を改訂する計画があることをサーバに知らせ、その後、サーバは、報告書を改訂するために報告書を要求する他の者に報告書を送信するのを拒否する(すなわち、報告書は、改訂者が改訂を行い又はロックを解除するまで改訂をロックアウトされる。)。ステップ１２３において、サーバは元の報告書、報告書のタイムスタンプ及び公証部の署名を公証部のワークステーションに送出する。ステップ１２４において、改訂者のワークステーションは、タイムスタンプをハッシュし、公証部の公開キーを用いて公証部の署名を解読して、公証部の署名を確認する。すなわち、ハッシュ及び署名の整合の解読がある場合、改訂者は、公証部の専用かぎにアクセスした者によって公証部の署名を発生させたこと及び署名が処理されたときにタイムスタンプに情報が存在したことを知る。タイムスタンプが作者の署名及び公証部の署名が処理された日時を含む時間を有するので、作者の署名がそのときに存在したことがわかる。ステップ１２５において、サーバステーションは、報告書をハッシュし、公証部の公開かぎを用いてタイムスタンプに

含まれる）作者の署名を解読し、作者の署名を確認する。すなわち、ハッシュ及び作者の署名の整合の解読がある場合、報告書は、作者の専用かぎにアクセスする者によって署名され、報告書は、それが署名されているために変更されない。

この第１の実施の形態の最終グループの図１ｄのステップ１３０において、改訂者は、報告書の改訂を作成し、改訂は、デジタル的に署名され、安全に格納され、かつ、デジタル的に公証される。ステップ１３２において、改訂者は、報告書の改訂を作成し、コマンドを入力して改訂をサーバに提出する。ステップ１３３において、ワークステーションは、改訂及び前のタイムスタンプを結合し、その結合をハッシュする。署名前にタイムスタンプを改訂に結合する目的は、元の文書との関係を証明できるようにすることである。代わりに又はタイムスタンプに加えて、改訂の履歴を表す他の情報を改訂に結合することができ、例えば、元の報告書の署名、元の報告書のハッシュ又はタイムスタンプの署名を結合に含めることができる。ステップ１３４において、ワークステーションは、改訂者（又はワークステーション）の専用かぎを用いて結合のハッシュを暗号化して、改訂者の署名を形成する。ワークステーションは、所望の場合には改訂、ハッシュ及び改訂者の署名を格納することができる。ステップ１３５において、ワークステーションは、改訂、改訂者の識別、改訂の題名、改訂者の署名をサーバに送出する。ステップ１３６において、サーバは、改訂及び元の報告書のタイムスタンプを結合し、その結合をハッシュし、改訂者の公開かぎを用いて改訂者の署名を復号化して改訂の起点及び保全性を確認する。ステップ１３７において、サーバは、解読された署名をハッシュと比較し、結果的に得られるハッシュ及び改訂者の署名の解読が整合する場合、サーバは、改訂が改訂者からのものであり、改訂が元の報告書に基づくものであり、かつ、改訂者が署名したために改訂及び署名が変更されないことを知る。ステップ１３８において、セキュアサーバは、改訂、改訂者のＩＤ、題名及び改訂者の署名を[illegible]として格納する。ステップ１３９において、サーバは、改訂者[illegible]タイムスタンプを公証局から得るとともに、改訂に関連するタイムスタンプ[illegible]。これは、元の報告書に対するステップ１１０で説明したのと[illegible]タイムスタンププロセスである

。この後、改訂の履歴を記録するのと同様にして最近の改訂に基づく将来の改訂が行われる。

図２ａ－２ｄは、改訂を確認する本発明の他の特定の実施の形態を示す。図２ａにおける第１グループのステップ１６０では、作者は、イメージを作成し、そのイメージをサーバに転送し、そのサーバは、作者に対してイメージを署名するとともにそのイメージを格納する。ステップ１６２において、作者はイメージャ（ｉｍａｇｅｒ）を操作してイメージを作成するとともに、イメージのセキュアサーバへの提出を開始する。イメージャを、ビジネスページスキャナや、医療用スキャナ（心電図／心血管撮影、超音波イメージャ、コンピュータ化軸方向Ｘ背っ断層写真術、磁気共鳴イメージャ、Ｘ線スキャナ）のようなイメージを発生させる装置又はイメージを形成する他の任意の方法とすることができ、イメージをビデオイメージ又は音声イメージとすることができる。ステップ１６３において、イメージャは、セキュアリンクを通じてイメージをセキュアサーバに転送する。その転送は作者又はイメージャ装置を識別する。サーバは、イメージャに対するシーケンス番号をリターンして、イメージに対する後のアクセスを容易にする。ステップ１６４において、サーバは、イメージャＩＤ及び作者ＩＤをイメージに結合し、その結合をハッシュしてイメージハッシュを発生させ、また、サーバは、スキャナＩＤ又は作者ＩＤをイメージのハッシュに結合して、イメージハッシュを発生させる。結合の既知の方法は、ＩＤをイメージハッシュに添付することＩＤ及びイメージハッシュの排他的論理和演算を有する。また、イメージャ又は作者は、イメージの起点を証明するのに用いることができる特定の専用／公開パスワード（かぎ）対を有し、イメージャＩＤ及び作者ＩＤをハッシング前にイメージに結合する必要がない。ステップ１６６において、サーバは、サーバの専用かぎ（又はサーバに格納された作者若しくはイメージャの専用かぎ）を用いて、識別をまた結合を確認し、イメージ署名を確認する。ステップ１６８において、サーバは、イメージ、イメージャＩＤ又は作者ＩＤ、イメージャに対するイメージシーケンス番号、イメージハッシュ及びサーバのイメージ署名を関連的に格納する。

図２ｂにおける第２グループのステップ１７０では、サーバは、イメージに対する公証部からタイムスタンプ及びタイムスタンプ署名を得る。ステップ１７２において、サーバは、公証部のホストネットワークとの接続を確立し、サーバのイメージ署名をホストに送出する。ステップ１７４において、ホストは、サーバのイメージ署名、受信時間、公証人ＩＤ、タイムスタンプのシーケンス番号（これは、イメージのシーケンス番号と異なる。）及びサーバＩＤを有するイメージタイムスタンプを形成する。ステップ１７５において、ホストはイメージタイムスタンプをハッシュし、ステップ１７６において、ホストは、公証部の専用かぎを用いてタイムスタンプハッシュを署名する。ステップ１７７において、ホストは、イメージタイムスタンプ及び公証部のイメージ署名を格納する。ステップ１７８において、ホストは、イメージタイムスタンプ及び公証部のイメージ署名を有するイメージ証明を送信する。ステップ１７９において、サーバは、イメージタイムスタンプをハッシュするとともに、公証部の公開かぎを用いて公証部のイメージ署名を復号化して、タイムスタンプ及び公証部の署名の保全性及び起点を確認する。ステップ１８０において、サーバは、イメージャに対するイメージシーケンス番号に関連する公証部のイメージ証明を格納する。

図２ｃにおける第３グループのステップ１９０では、サーバは、イメージを自動的に改訂するとともに、改訂の際に公証されたタイムスタンプを得る。ステップ１９２において、サーバは、イメージを損失データ圧縮する。例えば、ビットイメージを、ＪＰＥＧ圧縮によってビット減少イメージに圧縮し、音声イメージをＭＰＥＧ－２又はドルビー（Ｄｏｌｂｙ）ＡＣ３を用いて圧縮し、ビデオをＭＰＥＧ－２を用いて圧縮する。ステップ１９４において、サーバは、イメージャに対するイメージシーケンス番号に関連する圧縮及び他の関連の情報を格納する。ステップ１９６において、サーバは、例えば鉛いに識別することにおいて圧縮及び公証部のイメージ署名を結合する。ステップ１９８において、サーバは結合をハッシュして、圧縮ハッシュを発生させる。ステップ１９９において、サーバは、圧縮ハッシュを暗号化してサーバの圧縮署名を形成し、ステップ２００において、サーバは圧縮ハッシュ及び圧縮に関連するサーバの圧縮署名を格納する。

ステップ２０１において、サーバは、サーバの圧縮署名に対する公証部から圧縮証明(すなわち、圧縮タイムスタンプ及び公証部の圧縮署名)を得るとともに、圧縮に関連する圧縮証明を格納する。ステップ２０２において、サーバは元のイメージを削除して記憶スペースを保持することができるが、当然、これは、ユーザがもはや形成データすなわち元のイメージの起点を証明できないこと、又は圧縮が少なくともセキュアサーバから独立した元のイメージの積であることを意味する。特

にビデオの非圧縮イメージが結果的に生じるビデオの１００倍の容量を必要とするので、削除が必要となるおそれがあり、このような多量の容量を顧客が利用できないすなわち顧客に付与しない。また、元のイメージを、取り外し可能なテープ又は光媒体上で達成することができ、かつ、オフラインにし又は長時間保持するために送出することさえできる。

図２ｄにおける最終グループのステップ２１０では、ユーザはビュアー上で観察するためのイメージを要求し、格納されたイメージを、タイムスタンプ及び公証部の署名とともに提供し、その結果、ビュアーは、起点及び改訂の証明日を確認することかでき、少なくともセキュアサーバの記録に従って、改訂を元のイメージの積とする。ステップ２１２において、ユーザは、ビュアーを用いて圧縮イメージを要求する。ビュアーを、圧縮イメージをユーザに再生することができる任意の装置とすることができる。ビュアーは視覚的なディスプレイに限定されるものではなく、例えば、音声イメージを再生する拡声器とすることができる。ステップ２１３において、サーバは、イメージハッシュ、イメージＩＤ、イメージ圧縮、イメージと圧縮イメージの各々に対するタイムスタンプおよび公証部の署名とともに圧縮タイムスタンプを提供する。ステップ２１４において、ビュアーは、圧縮タイムスタンプをハッシュするとともに、公証部の公開かぎを用いて公証部の圧縮署名を解読して、圧縮タイムスタンプのデジタルタイム及び他の情報を確認する。ステップ２１５において、ビュアーは、イメージタイムスタンプをハッシュするとともに、公証部の公開かぎを用いて公証部のイメージ署名を解読して、イメージタイムスタンプを確認する。ステップ２１６に

おいて、ビュアーは、圧縮ハッシュ及び公証部のイメージ署名を結合するとともに、その結合をハッシュし、ステップ２１８において、ビュアーは、サーバの圧縮署名を解読するとともに、その解読をハッシュと比較して圧縮の起点及び保全性を確認する。また、ビュアーは、サーバのイメージ署名を解読するとともに、それをイメージハッシュと比較して、イメージャＩＤに関するセキュアサーバの記録をクロスチェックする。両タイムスタンプを確認した後、ビュアーはイメージタイムスタンプの時間を圧縮タイムスタンプの時間と比較して、これらの時間が非常に近接していることを確認する。ステップ２１８において、ビュアーはイメージを圧縮解除する。ステップ２２０において、ビュアーは、圧縮解除されたイメージ、イメージャＩＤ(又は作者のＩＤ)、イメージ送信時間及び圧縮時間をユーザに送信する。

図３ａ－ｃは本発明の他の実施の形態を示し、この場合、サーバは受信の際にビデオを自動的かつ即時に圧縮し、ビデオの受信及び圧縮に対して１個のタイムスタンプを得る。図３ａにおける第１グループのステップ２３０では、ビデオを形成するとともにそれをサーバに送信する。ステップ２３２において、作者は、ビデオイメージャを操作してビデオを形成するとともにビデオをサーバに送信する。イメージャを、ビデオカメラやマイクロホンのようなマルチメディア表示を形成する任意の装置とすることができる。ビデオは、ビデオイメージの他に音声チャネル及び他のデータを有することができる。好適には題名も形成する。ステップ２３３において、イメージャは先ず送信のためにビデオを圧縮する。例えば、イメージャは、ＭＰＥＧ－２又は他の簡単な損失圧縮法、好適には損失のない[illegible]。ステップ２３４において、イメージャは[illegible]第１圧縮をハッシュする。イメージャは、[illegible]のようなイメージハッシュを有するイメージャＩＤやイメージシーケンス番号のような他の情報もハッシュすることができる。ステップ２３５において、イメージャは、イメージャ（又は作者）の専用かぎを用いてハッシュを暗号化してビデオを署名する。イメージャは、サーバから受信の確認を得るまでビデオ、第１圧縮、ハッシュ及びイメージャの署名を格納する。ステップ２３６において、イメージャは、ビデオ題名

、第１圧縮及び署名をサーバに送信する。ステップ２３８において、イメージャはビデオを削除して、記憶領域を確保し、サーバからの受信を受信した後、イメージャはビデオの第１圧縮を削除する。第１圧縮をイメージャでも達成することができるが、一般的には、既に説明したように第１圧縮をサーバで達成するほうが便利である。

図３ｂにおける第２グループのステップ２４０では、サーバは、第１圧縮を受信し、確認し及び格納し、ビデオの第２圧縮を行うとともに、第２圧縮に対するタイムスタンプ及びタイムスタンプ署名を公証部から得る。ステップ２４１において、サーバは、ビデオの第１圧縮、イメージャの署名、題名、イメージャＩＤ

及び可能な場合には他の関連の情報を受信し、その受信をイメージャに送り返す。ステップ２４２において、サーバは、ビデオの第１圧縮をハッシュし、イメージャの公開かぎを用いてビデオイメージャの署名を解読し、かつ、その解読をハッシュと比較して第１圧縮の起点及び保全性を確認する。ステップ２４３において、サーバは、表題、作者のＩＤ、イメージャの署名及び第１圧縮のハッシュを関連的に格納する。ステップ２４４において、確認の直後に、サーバはビデオの第２圧縮を行う。ステップ２４５において、サーバは、ビデオの第１圧縮を行って、記憶スペースを確保し、かつ、オンライン記憶装置から第１圧縮を除去する。

ステップ２４６において、サーバは、題名、イメージャＩＤ、作者のＩＤ、イメージャ（又は作者）の署名及び第２圧縮を結合するとともに、その結合をハッシュする。ステップ２４７において、サーバは、サーバの公開かぎを用いて結合ハッシュを暗号化し、第２圧縮ビデオデータ、イメージャの署名を生成する。ステップ２４８において、サーバは、第２圧縮ビデオ、それに関連したサーバのビデオ署名、イメージャの署名及び関連の情報を格納する。ステップ２５０において、サーバは、サーバの署名に対して公証部からタイムスタンプ及び公証部の署名を得、公証部のタイムスタンプ及び署名を確認し、かつ、第２圧縮に関連する公証部のタイムスタンプ及び署名を格納する。

図３ｃにおける本実施の形態の最終グループのステップ２６０では、ビデオが

要求され、確認され及びディスプレイ上に表示される。ステップ２６２において、ディスプレイにいるユーザは、サーバからビデオを要求する。ステップ２６３において、サーバは、イメージャＩＤ、表題、第２圧縮、（サーバの署名を有する）公証部のタイムスタンプ及び公証部の署名をディスプレイに送信する。第１圧縮のハッシュ及びビデオイメージャの署名を送信して、ビデオの起点のクロスチェックを行うこともできる。ステップ２６４において、ディスプレイは、公証部の公開かぎを用いて公証部の署名を解読し、タイムスタンプをハッシュし、かつ、結果を比較してタイムスタンプを確認する。ステップ２６５において、ディスプレイは、既に説明したようにして結合及びハッシュを行って、第２圧縮ハッシュを形成し、サーバの公開かぎを用いてサーバの署名を解読し、かつ、これら結果を比較して第２圧縮の起点及び保全性を確認する。ディスプレイは、イメージャ

の署名及び第１圧縮ハッシュを受信し、イメージャの署名を解読し、結果を第１圧縮ハッシュと比較して、第１圧縮の起点に対するサーバの記録のクロスチェックを行うこともできる。ディスプレイは、第１圧縮のコピーを得ることなく第１圧縮の起点及び保全性を独立して確認することができない。ステップ２６６において、ビュアー（ディスプレイ）は第２圧縮を復号化して、圧縮解除されたビデオを形成する。最後に、ステップ２６７において、ユーザはディスプレイ上のビデオを観察する。ユーザは、作者ＩＤ、イメージャＩＤ、第２圧縮の形成時間及び公証部のタイムスタンプ情報のようなビデオについての他の情報を観察することもできる。

図１は本発明のネットワーク３００を示し、このネットワークは、複数のコンピュータノードをケーブル及び通信装置３０１の通信ネットワークによって互いに接続する。ネットワークノードは、ローカルサーバ３０２及び公証部３０３を有する。複数の作成局３０４－３１３を、通信ネットワークを通じてサーバに接続し、複数の観察局３１４－３２３も、通信ネットワークを通じてサーバに接続する。作成局は、Ｘ線や、テストデータや、走査や、ビデオ及び音声イメージや、マルチメディア表示のような文書を形成する装置と、文書をサーバに送信し、

サーバから文書を要求し、かつ、そのような文書を改訂する装置とを有する。観察局は、主にサーバからデジタル文書を要求するとともにその文書を観察するが、ノート及びコメントの追加のような文書を改訂するある制限された機能も有する。

図５において、図４の作成局３０４の詳細を示す。作成局は、電子メモリ３５３と通信する中央処理装置（ＣＰＵ）やはめ込まれたコントローラのようなプロセッサ３５２を有する。メモリは、プロセッサの動作を制御するプログラムと、作成局の周辺機器から入力及び／又は出力（Ｉ／Ｏ）回路３５４（ＩＯＣ）を通じて受信した情報を格納するとともに、ＩＯＣ３５５を通じてネットワークの他のノードから情報を送信し及び受信するバッファとを有する。周辺機器は、例えば、キーボード３５６と、マウス３５７のようなポインタと、ビデオカメラ３５８と、マイクロホン３５９と、スキャナ３６０と、ディスクメモリ３６１とを有する。

メモリは、ユーザと対話してバッファ３７１に格納された文書を発生させるとともに、文書をサーバに送信するプロセスを開始するプログラムモジュール３７０を有する。メモリは、１方向ハッシュを用いて文書をハッシュするとともにユーザ（発生者）の専用かぎ３９０又は局の専用かぎ３９０を用いてハッシュを暗号化して文書に対するデジタル署名を発生させるプログラムモジュール３７２を有する。メモリは、文書を署名に従ってサーバに送信するモジュール３７３も有する。プログラムモジュール３７５を用いて、文書、ハッシュ及び／又は署名を記憶装置３６１に格納することができる。ビデオイメージ及び音声イメージに対して、メモリは、動作ＪＰＥＧ又はＭＰＥＧビデオ、好適には損失のない圧縮方法のような圧縮形態にビデオを符号化するとともに他の文書のようなビデオの圧縮をバッファ３７１に格納するプログラムモジュール３７６を有する。

デジタル署名をサーバによって発生させる場合、作成システムは、サーバからバッファ３７１への文書署名、タイムスタンプ及びタイムスタンプ署名を受信するモジュール３７７と、署名を確認するとともにモジュールを初期化して文書署名、タイムスタンプ及びタイムスタンプ署名を記憶装置３６１に格納するモジュ

ール３７８とを有する。

作成局を、文書を改訂して改訂を発生させるのにも用いることができ、その改訂をサーバに戻すことができる。プログラムモジュール３７０を、サーバから文書を要求するために再検査者によって用いることができる。プログラムモジュール３７９は、文書、関連のタイムスタンプ及びサーバからの他の情報の受信の処理を行い、プログラム３８０は文書を証明する。本発明の上記実施の形態において、改訂局は、（上記）タイムスタンプ及び公証部の署名を受信する。モジュール３８０は、タイムスタンプをハッシュするとともに公証部の公開かぎ３９３を用いて公証部の署名を解読する装置３８３を有し、モジュール３８４は結果を比較して、タイムスタンプの起点を確認するとともに、デジタル時間を有するタイムスタンプの内容が変更されていないことを確認する。モジュール３８０のプログラム３８５は、文書をハッシュし、（タイムスタンプに含まれる）サーバ（又は作者の）署名を解読し、かつ、結果を比較してサーバの署名が文書用であるか否か決定するとともに、サーバによる署名のために文書が変更されていないことを確認する。さらに、文書が改訂である場合、元の文書のハッシュ、改訂に対するサ

ーバ、又は改訂する作者、の署名、及びタイムスタンプ及びその文書に対する公証部の署名を、サーバが送信するとともにモジュール３７９が受信し、その後、モジュール３８５は、元の文書に対するタイムスタンプを再び確認し、（タイムスタンプに含まれる）サーバの署名を解読し、かつ、結果を元の文書のハッシュと比較して、文書の起点を確認する。上記実施の形態の一部において、改訂者の署名又は以前の改訂者の署名のような情報を、サーバの署名を形成するためにハッシュし及び暗号化する前に文書に結合し、場合によっては、モジュール３８５は、解読した署名をこのようなアイテムの適切な組合わせのハッシュと比較する必要がある。その後、モジュール３８６を、ユーザと対話して文書を改訂するのに用いる。モジュール３８４は、以前のタイムスタンプに組み合わせた改訂をハッシュするとともに、ハッシュを信号化して改訂文書の署名を形成する。その後、改訂及び改訂の署名を、元の文書と同様にして格納し、送信し、セキュアし及

び確認する。

図６において、図４のサーバ３０２の詳細も示す。サーバは、電子メモリ４０３と通信する中央処理装置（ＣＰＵ）や埋込式コントローラのようなプロセッサ４０２を有する。メモリは、プロセッサの動作を制御するプログラムと、ネットワークから受信した情報並びに入力及び／又は出力（Ｉ／Ｏ）回路４０４（ＩＯＣ）を通じてネットワークに送信される情報を格納するバッファとを有する。ＩＯＣ４０４は、情報を送信するとともに、ネットワークに接続した他のノードから情報を受信する。サーバを、例えば、ネットワークの１個のＩＯＣを通じてローカルクライアントに接続するとともに他のＩＯＣを通じて他のネットワークの他のサーバ及び／又はリモートクライアントに接続したゲートウェイサーバとすることができる。ＩＯＣ４０５を、情報をディスク記憶媒体４０６に格納するのに使用し、それは、格納された情報を検索し、情報を記憶装置４０７に送信し、場合によってはその記憶情報を検索するのに用いられる。

メモリは、ＩＯＣ４０４を通じてネットワークとバッファ４２１の一部との間で文書をコピーするプログラムモジュール４２０を有する。上記実施の形態の一部において、サーバは、デジタル的に署名された文書を作成局から受信する。そのような場合、プログラムモジュール４２３は、文書上で一方向ハッシュを実行し、デジタル署名を解読し、かつ、結果を比較して、デジタル的に署名されているために文書が変更されていないこと及び文書の起点が正確であることを確認する。上記実施の形態の他の例において、サーバは、セキュアネットワークを通じて署名されていない文書を受信する。そのような場合、プログラムモジュール４２３は、文書をハッシュするとともに、サーバの専用かぎ又は発生者（若しくは作成局）の専用かぎ（この場合、セキュアサーバに保持されている。）を用いてハッシュを暗号化する。本実施の形態の他の例において、改訂者は、タイムスタンプ、タイムスタンプハッシュ又は公証部の署名を改訂に結合し、その結合をハッシュし、ハッシュを暗号化して改訂に署名する。したがって、改訂の署名は、改訂の起点及び保全性を確認するだけでなく、改訂が得られる元の文書を識別する。その後、改訂者は、改訂及び改訂の署名をサーバに送信する。そのような場

合、サーバのモジュール４２３は、改訂の署名を解読し、改訂を元の文書のタイムスタンプ及び他の任意の情報を改訂者と同様に結合し、その結合をハッシュし、かつ、結果を比較して、改訂の起点と、元の文書の起点と、署名のために改訂が変更されなかったことを確認する。

上記実施の形態の他の例において、サーバは、署名されていない改訂を受信し、その後、モジュール４２３は、元の文書の規定の表示の一部（以前の文書のハッシュ、以前の作者の署名、以前のタイムスタンプ、以前のタイムスタンプハッシュ又は以前のタイムスタンプの署名）及び改訂の起点の表示（改訂者のＩＤ、ワークステーションＩＤ）を改訂に結合し、その結合をハッシュし、サーバの専用かぎ又は発生者の専用かぎを用いてハッシュ（すなわち、文書の署名）を暗号化する。

上記実施の形態の他の例において、サーバは文書を受信し(署名されて異な場合にはプログラム４２３が文書を署名する。)、モジュール４２５は文書のタイムスタンプを得る。モジュール４２０は、自動的に文書を改訂し、元のタイムスタンプと改訂した文書との結合をハッシュし、ハッシュを署名する。その後、モジュール４２４は、自動改訂のための他のタイムスタンプを得る。

上記実施の形態の他の例において、モジュール４２２は文書を受信し、モジュール４２０は文書を署名し(、署名が文書とともに受信されない場合には)、改訂し駄文所に識別情報を結合し、モジュール４２０は自動的に文書を改訂し、結合をハッシュし及びハッシュを署名する。その後、モジュール４２４は、自動改訂に対する署名のタイムスタンプを得る。

文書を署名した後、プログラムモジュール４２５は、サーバの署名、サーバＩＤ、シーケンス番号及び（日付を含む）デジタル時間を有するタイムスタンプを形成する公証部に署名を送信し、モジュール４２０によって受信されたタイムスタンプ及びタイムスタンプの署名を戻す。その後、モジュール４２４は、タイムスタンプをハッシュし、(公証部の公開かぎを用いて)デジタル署名を解読して、識別された公証部からのタイムスタンプであるとともに署名のためにタイムスタンプが変更されていないことを確認する。

改訂された文書に対して、ＲＡＭ４０６（ハードディスク、ＤＶＤ，ＣＤ－ＲＯＭ）のスペースをセーブするために、プログラムモジュールは、アーカイビングとして既知のプロセスで、サーバから取り外される取り外し可能な記憶媒体(例えば、テープ)に文書の旧版をコピーする。記録された文書が要求されると、プログラム４２６は、記憶装置４０７にロードされる記録テープを有するとともに要求されたファイルをサーバに戻して格納する責任を負う。

図７において、図４の公証部３０３の詳細を示す。公証部は、電子メモリ４５３と通信する中央処理装置（ＣＰＵ）や埋込式コントローラのようなプロセッサ４５２を有する。メモリは、プロセッサの動作を制御するプログラムと、ネットワークから受信した情報並びに入力及び／又は出力（Ｉ／Ｏ）回路４５４（ＩＯＣ）を通じてネットワークに送信される情報を格納するバッファとを有する。ＩＯＣ４５４は、情報を送信するとともに、ネットワークに接続した他のノードから情報を受信する。ＩＯＣ４５５を用いて、タイムスタンプ及びタイムスタンプの署名をディスク４５６上に格納する。

メモリは、文書の署名の受信並びにタイムスタンプ及びタイムスタンプの署名の送信を制御するプログラムモジュール４７０を有する。公証部の署名が要求される場合、プログラム４７０は、ネットワークからバッファ４７１の一部に文書の署名をコピーする。タイムスタンプ及び公証部の署名を発生させた後、プログラム４７０は、バッファ４７１の一部からネットワークにコピーする。プログラムモジュール４７２は、サーバの署名をバッファから読み出し、サーバの署名、サーバの署名を受信した（任意の時間形式の）時間、公証人ＩＤ及びシーケンス番号を有するタイムスタンプを形成する。その後、モジュール４７２は、タイムスタンプをハッシュするとともに、公証人の専用かぎを用いてハッシュを暗号化して、公証人のタイムスタンプの署名を形成する。その後、モジュール４７３は、タイムスタンプ及び公証人の署名の送信の準備を行い、証明送信をバッファ４７１に格納し、公証人の証明を顧客に戻すようにモジュール４７０を始動させる。プログラムモジュール４７４は、タイムスタンプ及びタイムスタンプの署名をタイムスタンプ署名記録とともにＩＯＣ４５５を通じてハードディスクドライブ

４５６にもコピーする。

タイムスタンプの署名の確認の識別が要求されると、要求は、文書の署名、タイムスタンプ、タイムスタンプの署名又はシーケンス番号を提供する。公証部は、記憶装置４５６から証明（タイムスタンプ及び公証人の署名）を検索するモジュール４７６を有し、識別要求で提供された情報を記録中の情報と比較するとともに情報が整合したか否かを決定するモジュール４７７とを有する。その後、モジュール４７８は、タイムスタンプの記録及び／又は比較の結果の送信を準備して情報を証明するとともに、バッファ４７１の応答を格納し、モジュール４７０はその応答を送信する。

図８は、プログラマブルコンピュータ装置５００及びそのようなプログラマブルコンピュータをプログラムする種々の装置の一例を示し、それらは全て既知である。コンピュータ装置を、プログラムされた構造を有する不揮発性メモリ（例えば、ＲＯＭ，ＰＲＯＭ，ＥＥＰＲＯＭ、フラッシュメモリ、バッテリ内蔵ＳＲＡＭ）をプログラマブルコンピュータに接続し又はプログラマブルコンピュータのメモリに適用することができるプログラマブルコンピュータに信号を供給してプログラムされた構造を設けることによって、プログラムすることができる。インターネットサーバのような他のコンピュータ装置５０１を通信装置５０２を介して装置５００に接続して、プログラミング装置５００に対する信号を発生させることができる。装置５０２を、銅又は光ケーブルや、イーサネット、ＡＲＣネット、トークンリング等の無線、赤外線ネットワークや、モデム及び電話回路網

とすることができる。メモリドライブ５０３は、統合媒体５０４を有することができ、装置５００に取り外し自在に取り付けることができ、又はドライブ５０３を装置５００に統合するとともに、それが取り外し自在のコンピュータ媒体５０４から信号を受信することができる。装置５００は、ユーザインタフェース及びプログラム入力モジュール５０６を有することができ、書き込まれたマテリアルを設けることができる。ユーザは、キーボードや、テキストスキャナや、マイクロホンや、カメラや、バーコードリーダのようなユーザインタフェースの装置（図示せず）を用いて信号を入力することができる。装置５００から発生した信号

を、揮発性メモリで後に呼び出すために記憶装置５０３にコピーし、又はプログラムされた装置をメモリに設けるために不揮発性メモリ５０８に格納する。装置を、プログラムされた不揮発性メモリを設けることによってプログラムすることもできる。装置５００は、ＰＣフラッシュメモリのような不揮発性メモリを有するカートリッジ５１０を接続してプログラムされた装置を設けることができるスロット５０９を有することができる。装置５００は、不揮発性パッケージ５１２を挿入してプログラムされた装置を設けることができるソケット５１１を有することができる。装置５００を、一体の不揮発性メモリ５０８を用いて製造して、プログラムされた装置を設けることができる。プログラムされた構造は、コンピュータ処理を行うためにプログラマブルコンピュータのマイクロプロセッサ５１３及びＩ／Ｏプロセッサ、例えば５１４を制御するメモリにプログラム及び他のデータを有する。コンピュータ装置を、ワークステーション、モデム、ＰＣカード又は他のアップグレード可能なソフトウェア構成要素とすることができる。コンピュータ装置をプログラムする他の十分既知の方法を用いることもできる。

本発明は、上記実施の形態に限定されるものではなく、幾多の変更及び変形が可能である。

【図1】

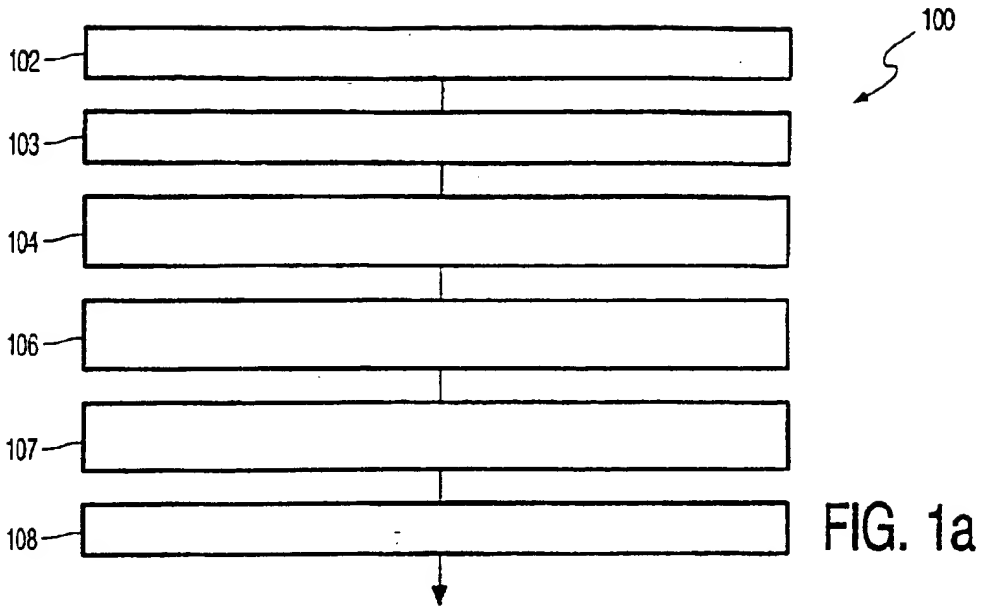

FIG. 1a

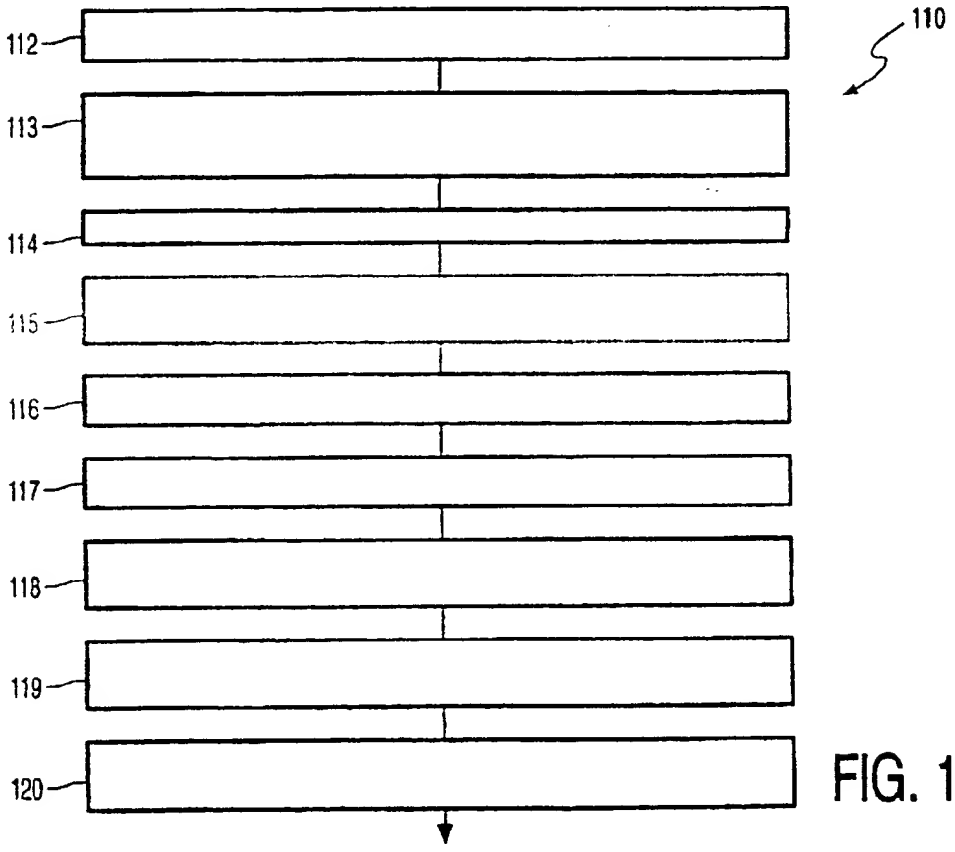

FIG. 1b

【図１】

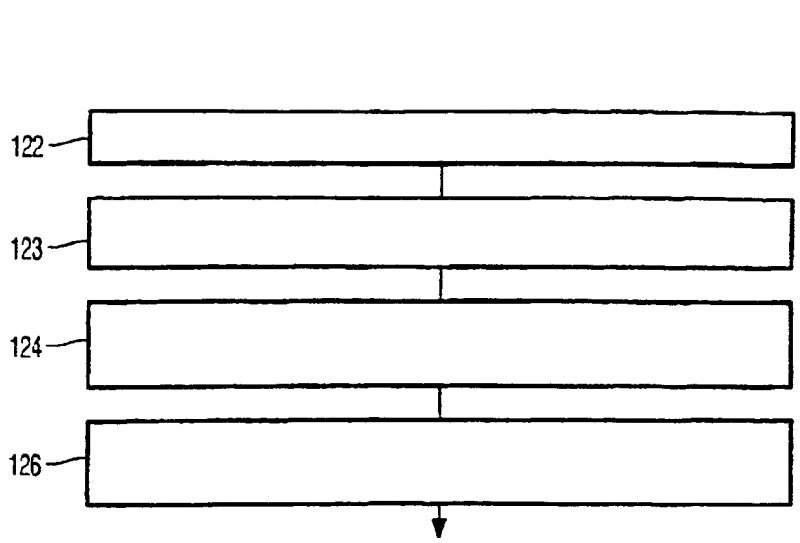

FIG. 1c

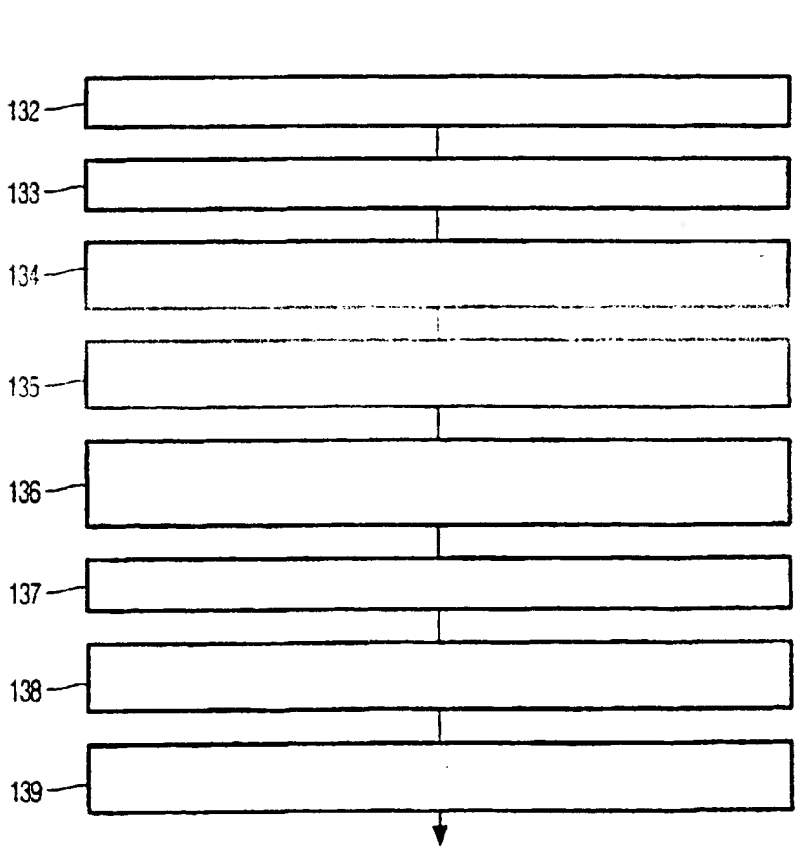

FIG. 1d

【図２】

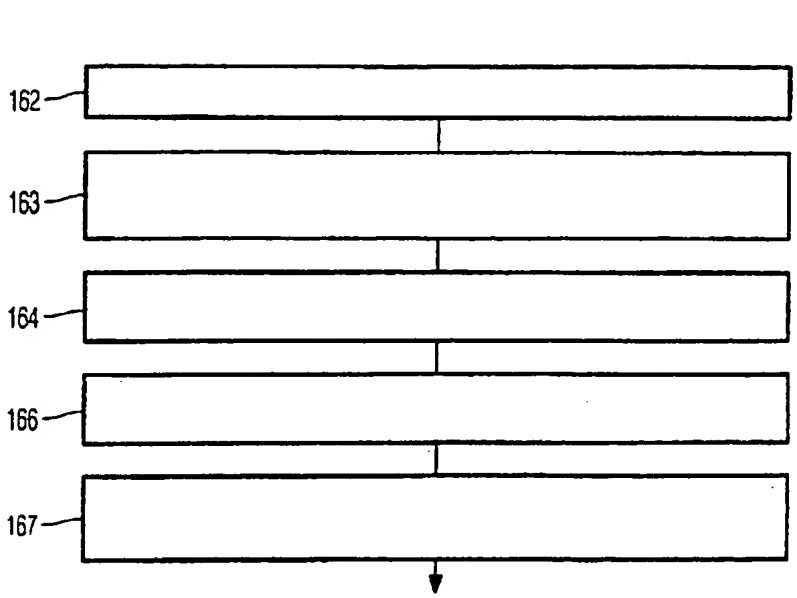

FIG. 2a

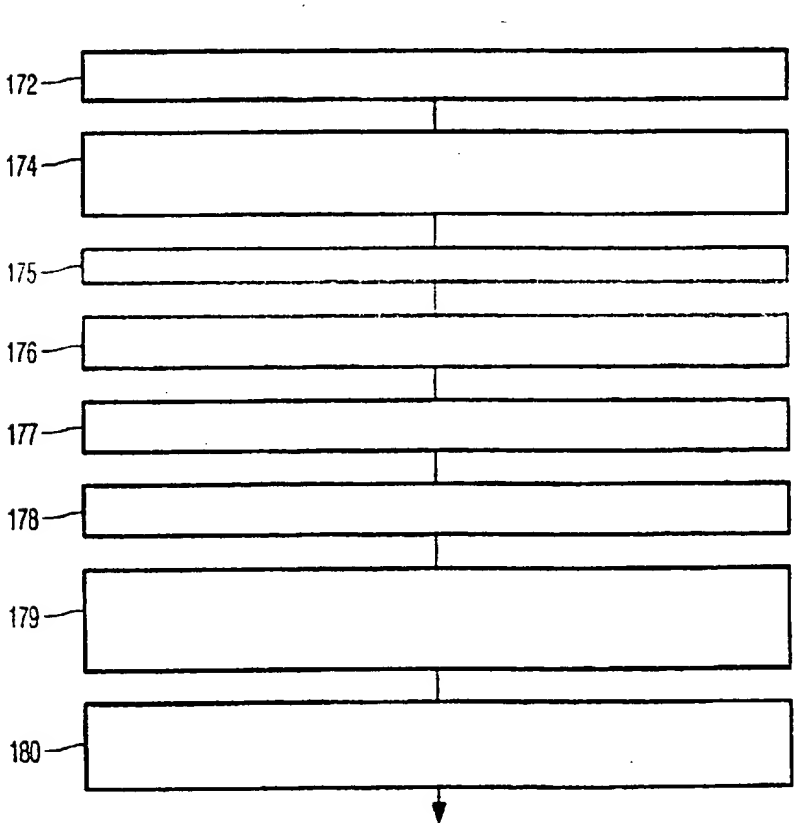

FIG. 2b

【図２】

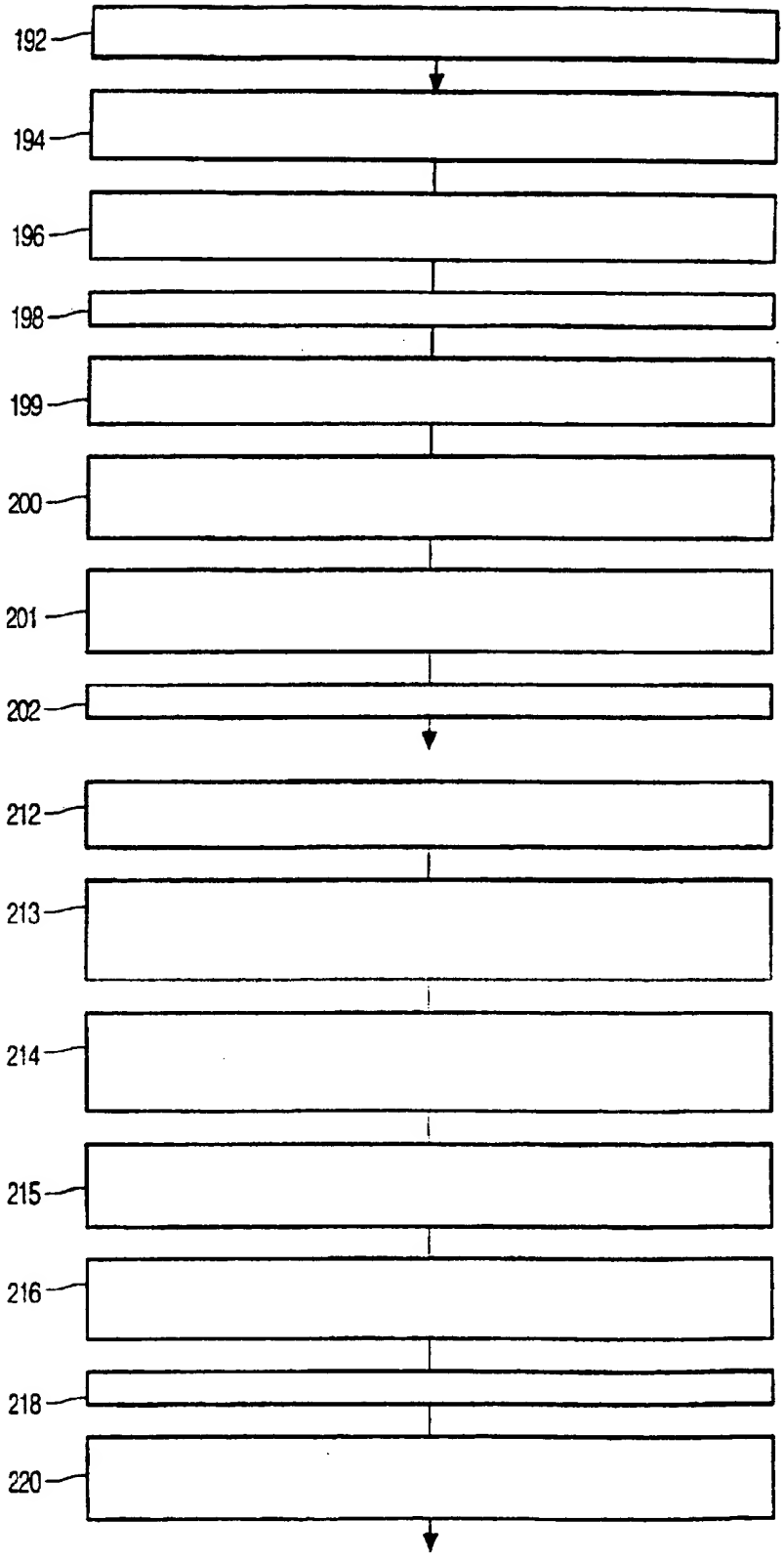

FIG. 2c

FIG. 2d

【図3】

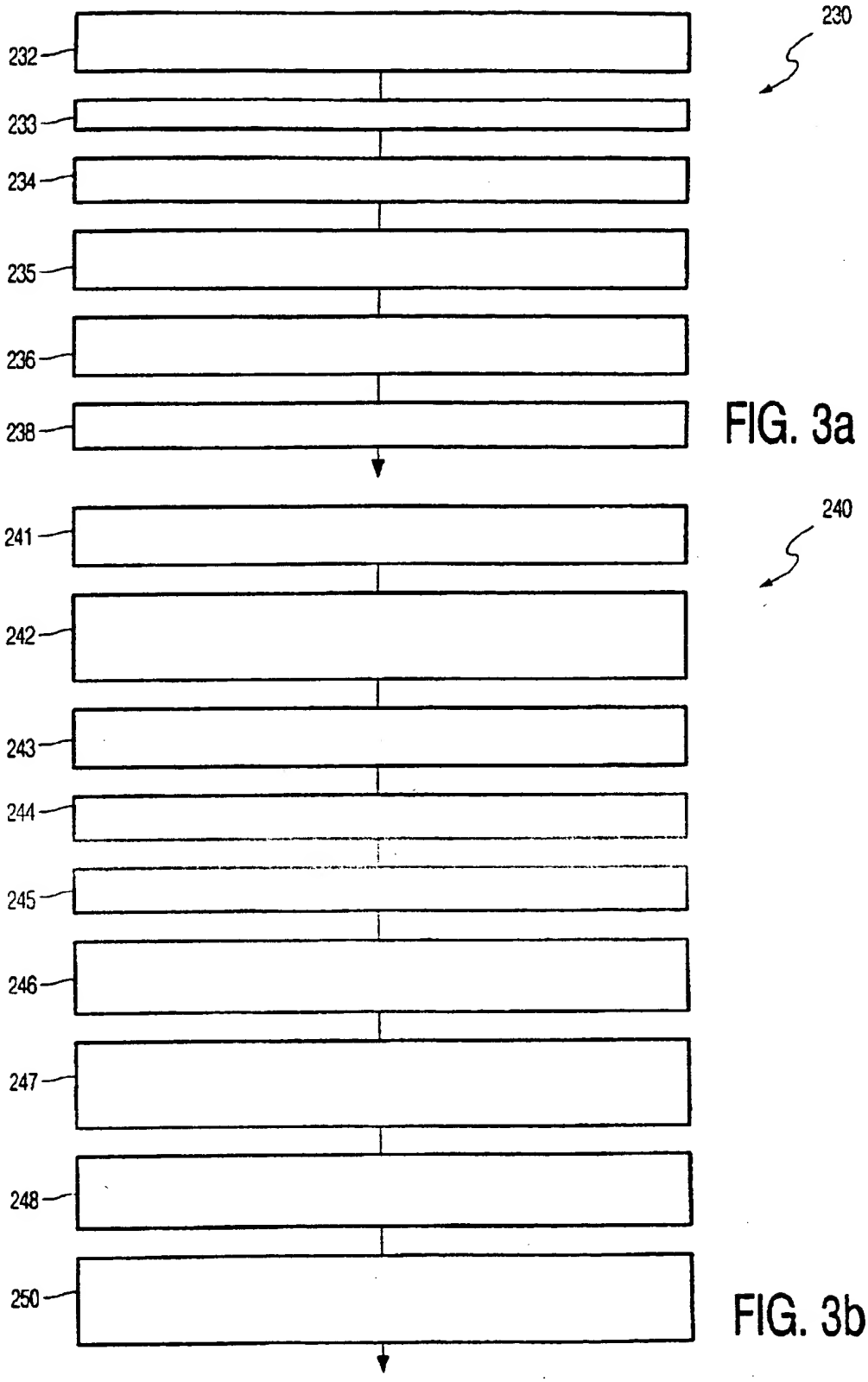

FIG. 3a

FIG. 3b

【図３】

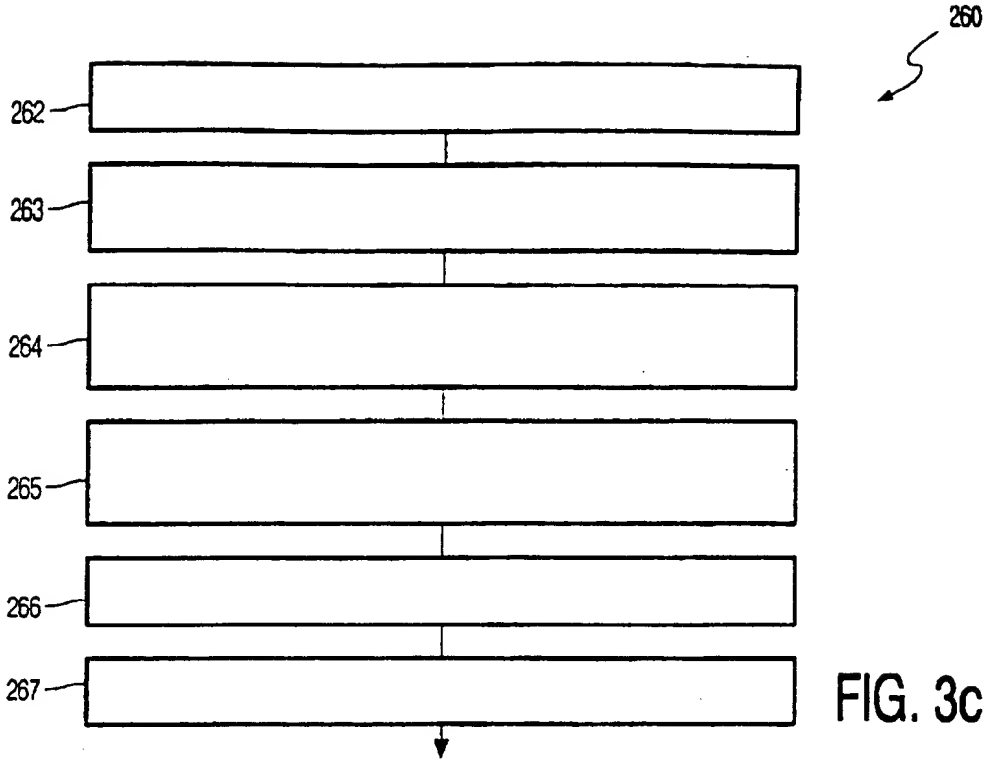

FIG. 3c

【図４】

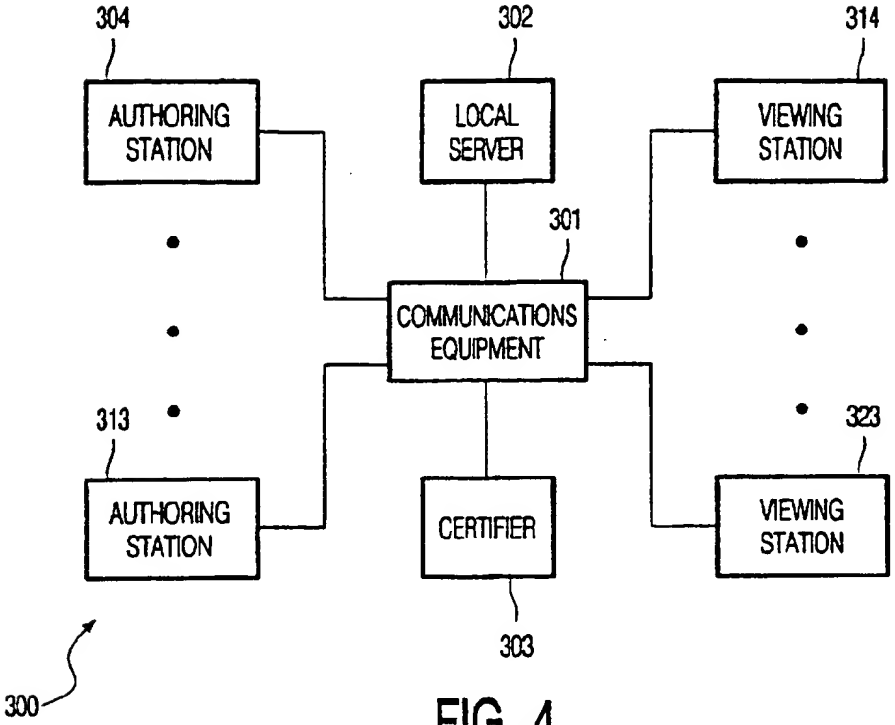
304
302
314
AUTHORING STATION
LOCAL SERVER
VIEWING STATION
301
COMMUNICATIONS EQUIPMENT
313
323
AUTHORING STATION
CERTIFIER
VIEWING STATION
303
300

FIG. 4

【図５】

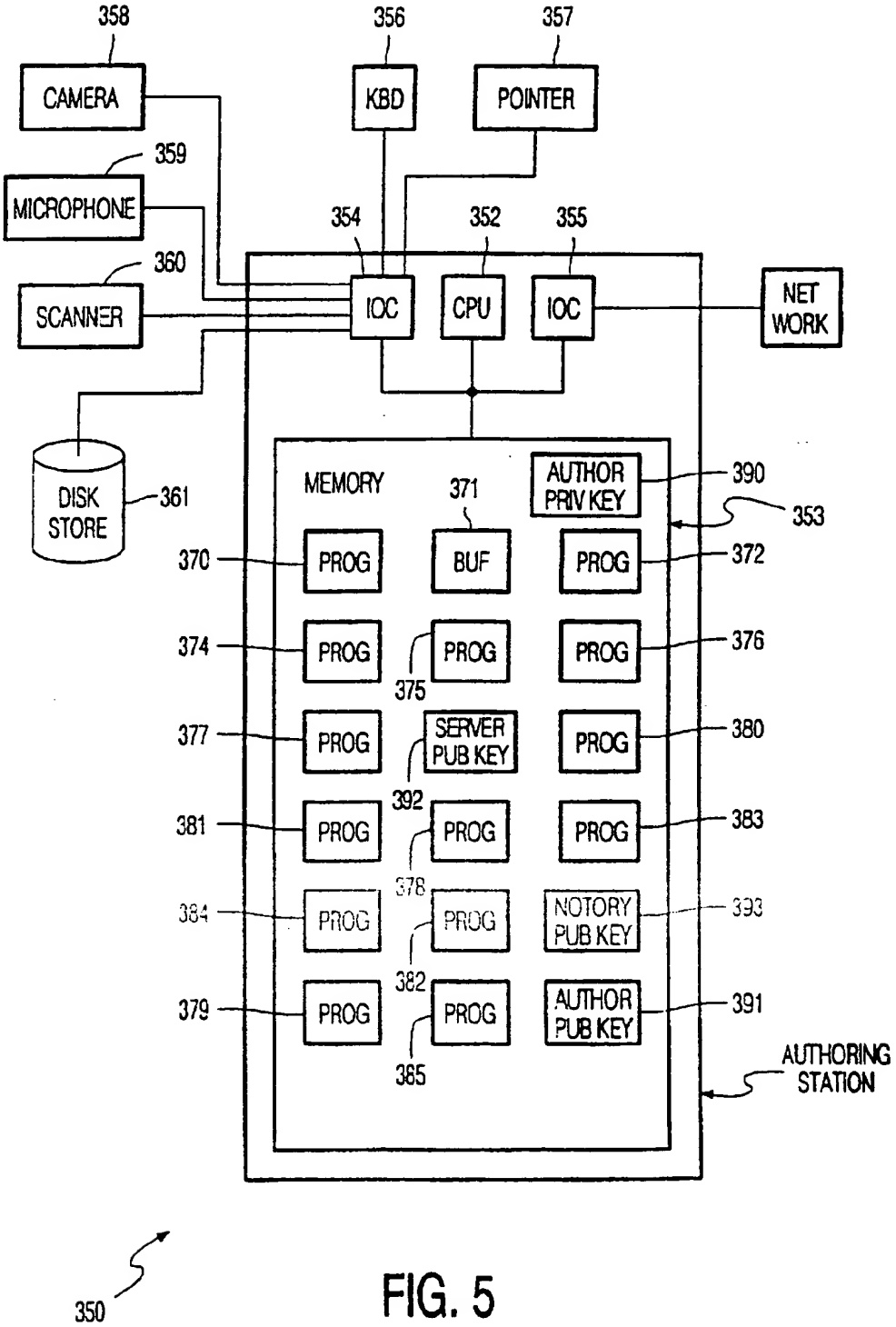
358
CAMERA
356
KBD
357
POINTER
359
MICROPHONE
354
352
355
360
SCANNER
IOC
CPU
IOC
NET WORK
DISK STORE
361
MEMORY
371
AUTHOR PRIV KEY
390
353
370
PROG
BUF
PROG
372
374
PROG
PROG
PROG
376
375
377
PROG
SERVER PUB KEY
PROG
380
392
381
PROG
PROG
PROG
383
378
384
PROG
PROG
NOTORY PUB KEY
393
382
379
PROG
PROG
AUTHOR PUB KEY
391
365
AUTHORING STATION
350

FIG. 5

【図６】

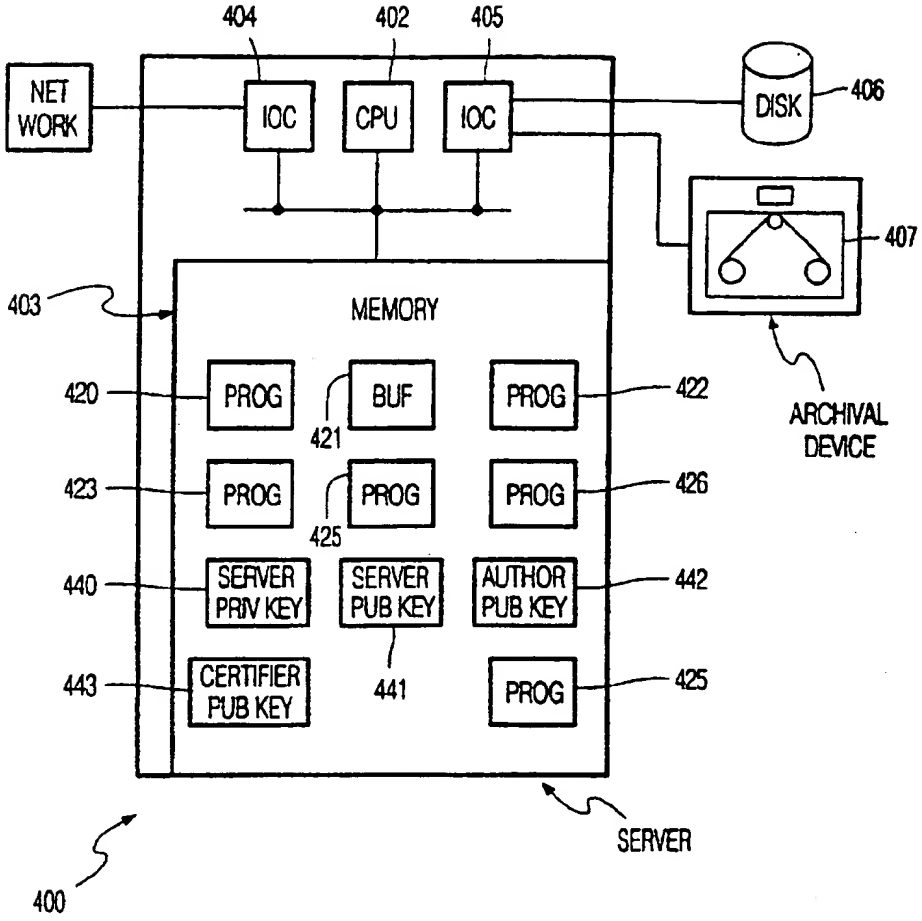
404
402
405
NET WORK
IOC
CPU
IOC
DISK
406
407
403
MEMORY
420
PROG
BUF
421
PROG
422
ARCHIVAL DEVICE
423
PROG
PROG
425
PROG
426
440
SERVER PRIV KEY
SERVER PUB KEY
AUTHOR PUB KEY
442
443
CERTIFIER PUB KEY
441
PROG
425
SERVER
400

FIG. 6

【図７】

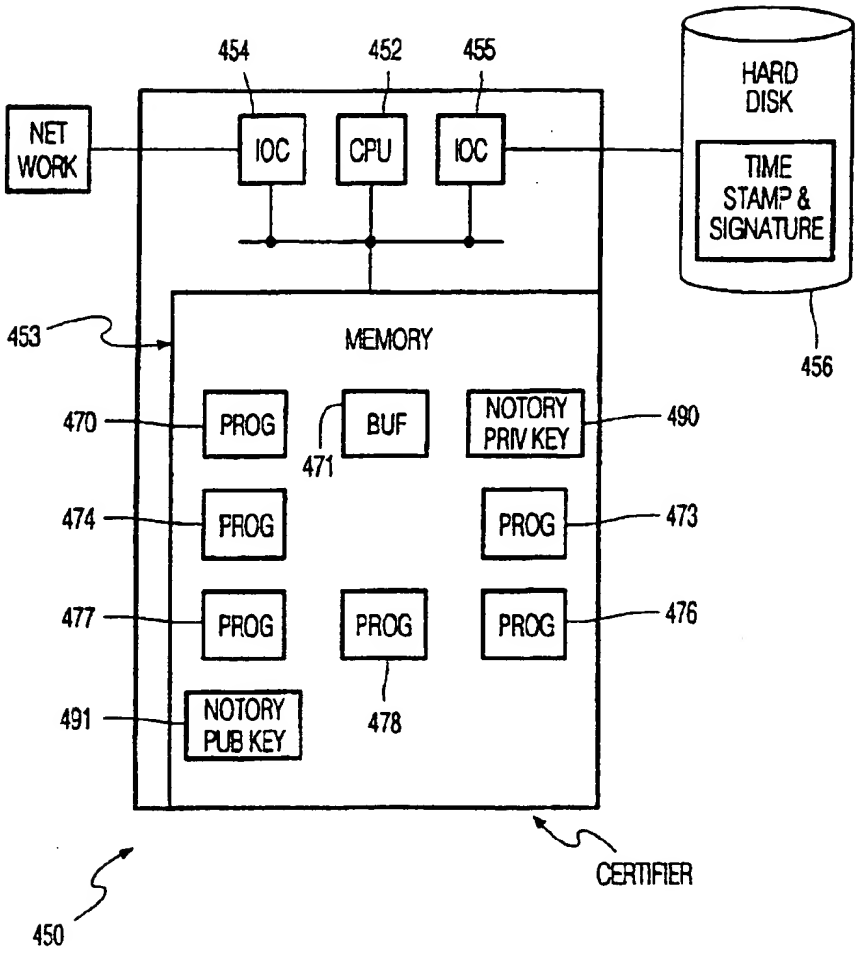
454
452
455
HARD DISK
NET WORK
IOC
CPU
IOC
TIME STAMP & SIGNATURE
456
453
MEMORY
470
PROG
BUF
471
NOTORY PRIV KEY
490
474
PROG
PROG
473
477
PROG
PROG
PROG
476
491
NOTORY PUB KEY
478
CERTIFIER
450

FIG. 7

【図8】

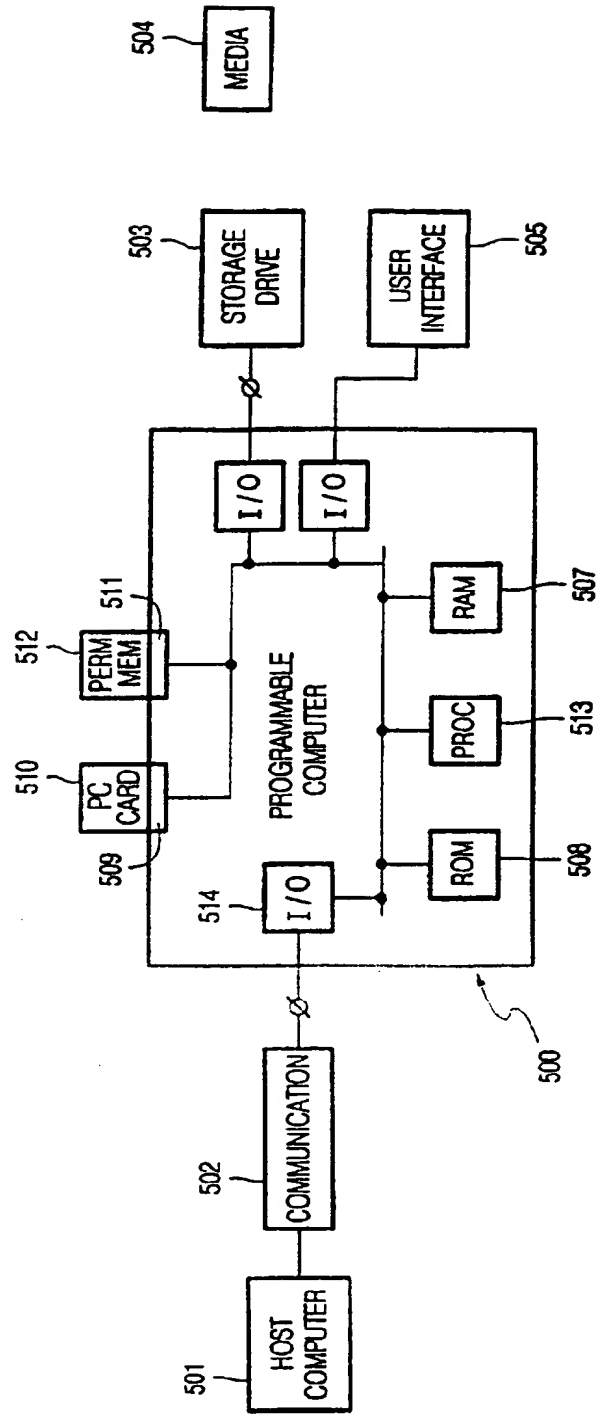
504
MEDIA
503
STORAGE DRIVE
505
USER INTERFACE
I/O
I/O
511
512
PERM MEM
510
PC CARD
509
PROGRAMMABLE COMPUTER
RAM
507
PROC
513
ROM
508
514
I/O
500
502
COMMUNICATION
501
HOST COMPUTER

FIG. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 98/02120

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5136646 A (STUART A. HABER ET AL), 4 August 1992 (04.08.92), abstract --	1-22
A	US 5659616 A (FRANK WELLS SUDIA), 19 August 1997 (19.08.97), abstract --	1-22
A	EP 0624014 A2 (FISCHER, ADDISON M.), 9 November 1994 (09.11.94), abstract --	1-22
A	EP 0586022 A1 (FISCHER, ADDISON M.), 9 March 1994 (09.03.94), abstract -- --------	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 July 1999	22-07-1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bengt Romedahl/cs Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

01/07/99

International application No.
PCT/IB 98/02120

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5136646 A	04/08/92	CA 2088371 A,C	03/02/92
		EP 0541727 A	19/05/93
		JP 6501571 T	17/02/94
		WO 9203000 A	20/02/92
US 5659616 A	19/08/97	AU 698454 B	29/10/98
		AU 3715695 A	16/02/96
		CA 2194475 A	01/02/96
		CZ 9700115 A	17/09/97
		EP 0771499 A	07/05/97
		JP 10504150 T	14/04/98
		NO 970084 A	10/03/97
		TR 970079 A	00/00/00
		WO 9602993 A	01/02/96
EP 0624014 A2	09/11/94	AU 666424 B	08/02/96
		AU 5778194 A	17/11/94
		CA 2120665 A,C	06/11/94
		EP 0770953 A	02/05/97
		EP 0841604 A	13/05/98
		JP 7254897 A	03/10/95
		US 5422953 A	06/06/95
EP 0586022 A1	09/03/94	SE 0586022 T3	
		AT 113429 T	15/11/94
		AT 150605 T	15/04/97
		AU 620291 B	13/02/92
		AU 4242589 A	13/09/90
		CA 2000400 A,C	07/09/90
		DE 69013541 D,T	09/03/95
		DE 69030268 D,T	26/06/97
		DK 386867 T	03/04/95
		EP 0386867 A,B	12/09/90
		SE 0386867 T3	
		ES 2036978 T	01/01/95
		ES 2098651 T	01/05/97
		GR 93300050 T	30/06/93
		JP 2291043 A	30/11/90
		US 5005200 A	02/04/91
		US 5214702 A	25/05/93